WELCOME TO THE AGE OF "BRING YOUR OWN NETWORK"

Security First: Cree Lighting, IoT Cybersecurity and Connected Lighting Networks

CREE LIGHTING

A DECADE AGO IT WAS BYOD. NOW IT'S LITERALLY "BRING YOUR OWN NETWORK".

The rapid adoption of IoT devices in corporate and industrial settings is being talked about in terms of connectivity statistics that reach numbers in the billions. Everything from toilet paper dispensers to the company coffee pot is getting sensored-up and ready to chatter on the Internet.

Even if the IoT revolution hasn't arrived at your doorstep yet, you know it's coming. What may surprise you is where it's likely to show up first – in the LED light fixture right above your head.

Here's what you should know before engaging with lighting designers, vendors and engineers.

HOW LIGHTING CONTROL SYSTEMS BECAME CONNECTED NETWORKS

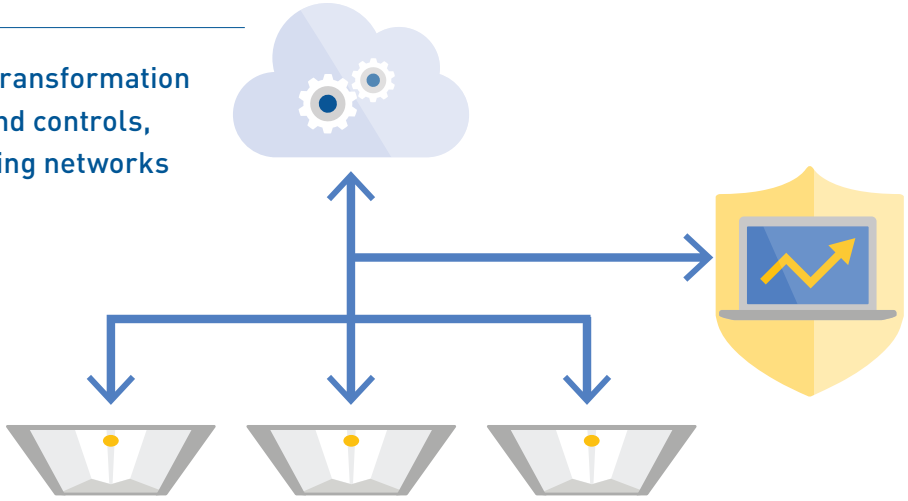
Intelligent controls for light fixtures (also called luminaires) have been around since the days of analog electronics. LED lighting has accelerated a transformation from analog to digital devices and controls, making the introduction of lighting networks a logical next step.

The first lighting control networks were standalone: isolated from enterprise networks and the Internet, and presenting no real cybersecurity concerns. But as companies grasped the potential for an intelligent lighting control network to also optimize space occupancy, fine-tune HVAC load and interact with other building systems — potentially lowering energy costs by as much as 70% — lighting manufacturers began offering connected lighting control networks.

Many of these vendors rushed their new lighting control networks to market, overlooking an important implication of interconnectivity: a lighting network connected to enterprise networks or the Internet requires enterprise-level security.

This isn't surprising: many traditional lighting companies were founded in the age of tungsten filaments and still approach LED lighting networks saddled with an "analog" mindset. As a result, a survey of networkable lighting control systems reveals that many lack basic security practices and protocols. Others apparently address security as an afterthought bolted on late in the game.

LED lighting has accelerated a transformation from analog to digital devices and controls, making the introduction of lighting networks a logical next step.



CREE LIGHTING'S BENCHMARK ISN'T TRADITIONAL LIGHTING. IT'S IT.

Cree Lighting brings an inherent advantage in this regard: our company is a "digital native," expressly created at the heart of the Internet revolution to innovate and manufacture LED lighting.

Our goal is to deliver cybersecurity in line with what you expect from any leading technology provider. With that in mind, we built the SmartCast Intelligence Platform™ around the security principles and practices we knew you'd want to see:

- Designed from inception to be secure under a rigorous BSIMM9 framework
- Leverages secure, open technologies subject to peer scrutiny
- Adheres to IT industry best practices and security standards
- Minimizes data vulnerability in motion or at rest
- Employs third-party penetration testing by prominent cybersecurity consultants

By engineering cybersecurity into the core of the product, we were able to implement IT best practices to secure endpoints, communications paths, servers, processors, databases and data. The result is a simple, open platform for interoperability with virtually limitless scalability and extensibility – all securely provisioned.

TOP 10%

In recently completed independent penetration testing, SmartCast® Technology cybersecurity was ranked among the top ten percent of all technology companies tested, a list that includes the leading technology brands that you use every day.

SMARTCAST INTELLIGENCE PLATFORM™

HARDWARE

- SmartCast-enabled LED lighting products, sensors and communication devices
- High LPW LEDs combined with basic control
- Better light

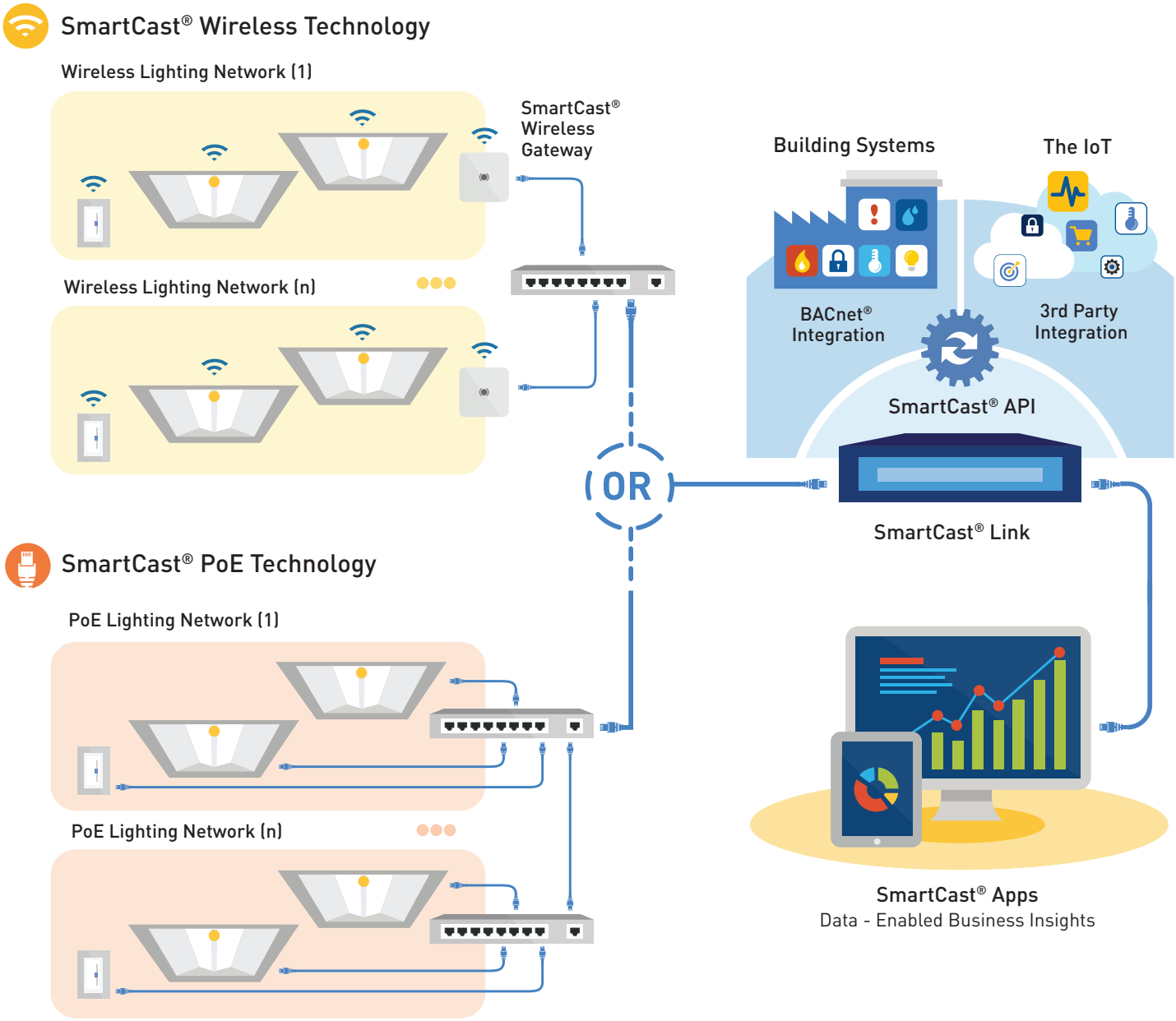
SOFTWARE

- Data collection and networking
- Software-driven analytics and decision guidance
- Open API enables simplicity, extensibility and interoperability
- Third party deployment

SERVICES

- Simple installation and commissioning
- Technical support
- Customer portal and community
- Software and security updates

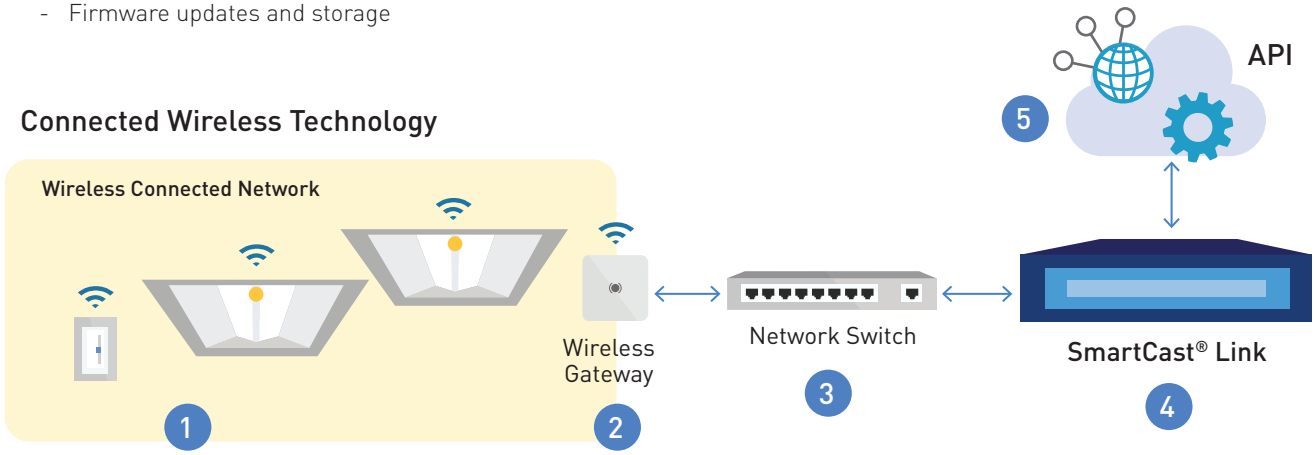
SmartCast® luminaires and wall switches act as endpoints, providing controlled light and gathering data from sensors. Sitting between the lighting network and the corporate network, SmartCast Link™ provides administrative control via a highly intuitive GUI and offers secure connectivity to outside networks to deliver value beyond lighting. SmartCast Link™ acts as a security arbiter: enterprise cybersecurity standards are rigorously applied and no packets pass directly from one network to the other. An embedded x86 appliance or virtual machine, SmartCast Link™ collects sensor data, exposes a RESTful API, provides a data analytics platform, and hosts web applications for managing energy usage, BACnet® connectivity and occupancy/vacancy analytics.



1. ENDPOINT AND LIGHTING NETWORK SECURITY

The endpoints in a lighting control network are the light fixtures. Each Cree Lighting SmartCast®-enabled luminaire collects data from multiple on-board sensors, transmits that data to SmartCast Link™, and receives commands from SmartCast Link™ in return. Luminaires in a SmartCast® Wireless network communicate with the SmartCast® Wireless Gateway via a lightweight mesh wireless network. Luminaires in a SmartCast® Power over Ethernet network communicate with the lighting network server via an Ethernet connection. All SmartCast luminaires encrypt all data using AES-128 block encryption.

- SmartCast® luminaires encrypt all data in motion and all data at rest
- Multiple AES-128 keys are used for protecting:
  - Device-to-device negotiation
  - Wireless data transfer
  - Firmware updates and storage



2. SMARTCAST® WIRELESS GATEWAY SECURITY

The SmartCast® Wireless Gateway securely connects up to 250 SmartCast® Wireless luminaires to SmartCast Link™. A single Ethernet cable carries both data and power to the device.

- SmartCast® Wireless Gateway encrypts all data in motion and data at rest
- SmartCast® Wireless Gateway uses AES-128 for local data encryption and communication with luminaires
- Communications between the SmartCast® Wireless Gateway and the SmartCast Link™ are protected through Mutual TLS
  - Mutual TLS requires that the SmartCast Link™ presents a Private Key Infrastructure (PKI) server certificate to validate that it is in fact a Cree Lighting SmartCast Link™
  - SmartCast® Wireless Gateway must also present a PKI client certificate to prove that it is a Cree Lighting SmartCast® Wireless Gateway
- SmartCast® Wireless Gateway uses RSA 2048 (longer key length, thus better encryption) for communication with the SmartCast Link™
- SmartCast® Wireless Gateway's SecureConnect functionality allows the Configuration Tool (CT) to generate an AES 128-bit Cree Lighting Encrypted File (CEF) that is manually transferred to a PC and uploaded to a SmartCast Link™.

3. SMARTCAST® NETWORK SWITCH SECURITY

While the Ethernet switch isn't provided by Cree Lighting, our recommended switches are produced by one of the world's leading providers of secure networking hardware, switches and routers. Corporate IT departments are of course welcome to provide their own Ethernet hardware.

4. SMARTCAST LINK™ SECURITY

The SmartCast Link™ platform has gone through an extensive hardening exercise. The platform has been independently subjected to penetration testing and re-testing by one of the industry's most respected cybersecurity firms.

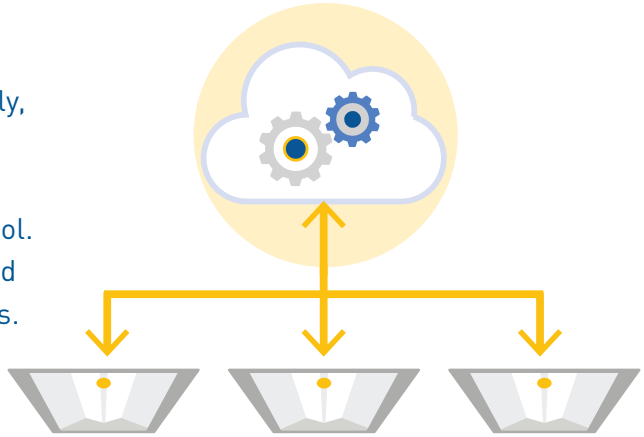
SmartCast Link™ employs an operating system purpose-built for security in a modern distributed infrastructure, designed to support large-scale clusters while enabling lean operational overhead.

- The SmartCast Link™'s OS relies on an immutable filesystem, meaning system files are always read-only. When the SmartCast Link™ receives an OS update, the entire filesystem is replaced, which (in conjunction with the filesystem's immutability) protects from latent malware intentionally introduced to the system. System administrators are alerted of available OS updates and security patches so they can manage the process and schedule the brief downtime required.
- Databases used on the SmartCast Link™ platform require authentication from other on-platform services. In the event that a service is compromised, the attacker must still have credentials to access data in any of the databases.
- SmartCast Link™ uses an OS-sharing virtualizer for efficient service containerization, minimizing the potential attack surface and shielding functionality from other services. This isolation ensures services can only communicate with those other services they are authorized to reach.
- SmartCast Link™ requires all user sessions to use HTTPS. HTTP requests are redirected HTTPS, ensuring every user session employs a secure, encrypted connection.
- SmartCast Link™ communicates with the SmartCast® Wireless Gateway via Mutual TLS (see above).
- All user credentials (user IDs and passwords) stored on the SmartCast Link™ are stored in a "secrets engine", provided by a third-party and designed to protect secrets. Local passwords are stored using a 32-bit salted PBKDF2 @ 1000 iterations. This protects against brute force attacks using GPUs, which are increasingly employed in such attacks as they are magnitudes faster than CPUs at parallelizing mathematical operations (such as calculating hashes).
- Only the authentication service on the SmartCast Link™ has the credentials to query or write to the secrets engine. Default password requirements include a minimum length of 8 characters, 1 upper case letter, 1 number and 1 special character. These requirements are fully configurable by the administrator for more stringent constraints.
- SmartCast Link™'s Trusted Platform Module (TPM) 2.0, an on-board secure cryptoprocessor, is responsible for generating security-related random numbers. The TPM is also leveraged for storage of the platform's endorsement key.
- SmartCast Link™'s SecureBoot technology prevents the introduction of malicious software. System firmware checks that the system boot loader is signed with a cryptographic key authorized by the firmware and rejects unsigned or malicious software.

5. SMARTCAST LINK'S APPLICATION PROGRAMMING INTERFACE (API) SECURITY

- The SmartCast Link™'s API is protected with API keys which must be issued by the SmartCast Link™ and authenticated with each client request. These unique tokens provide an additional level of security over basic authentication.
- SmartCast Link™'s Role-Based Access Control (RBAC) determines the level of administrative function or "role" associated with each API key. Each key can be individually assigned levels of access, such as "read," "write" or "admin."

Cree Lighting's first-gen lighting network was the industry's first self-commissioning lighting network: hundreds of luminaires talked to each other wirelessly, configured themselves into lighting groups based on sophisticated algorithms, and provided fingertip control to an operator via a handheld configuration tool. And it did all this with an intuitive simplicity that belied the complexity and cost of traditional lighting controls.



CREE LIGHTING'S COMMITMENT: CYBERSECURITY IT CAN TRUST

Even before designing the first SmartCast® network, Cree Lighting recognized that SmartCast® Technology would one day serve as an open and interoperable IoT platform connected to other networks. That meant creating a secure architecture to protect data and access from the ground up.

We have no doubt that the practices, technologies and standards associated with IoT-enabled LED lighting will continue to rapidly evolve. As they do, we'll continue to set the standard for secure, open, interoperable LED lighting networks. With Gartner predicting more than 20 billion Internet-connected devices by 2020, we think you'll have enough on your hands without worrying about the cybersecurity of your LED lighting. If you specify a Cree Lighting connected lighting solution, you won't have to.

If you require more details, your Cree Lighting sales representative can give you direct access to our technology

[1] Solid-State Lighting R&D Plan, June 2016; U.S. Department of Energy

MORE ABOUT THE CREE LIGHTING DIFFERENCE

The evolution of LED lighting has proceeded at a breakneck pace since Cree Lighting introduced the first commercially viable LED luminaires in 2007, so the disruptive innovation and abrupt transformation now seen in the IoT ecosystem is familiar territory for Cree Lighting.

When we introduced our first-generation SmartCast® lighting network in 2014, it was hailed by the US Department of Energy[1] as a model for future lighting networks. By adjusting light levels based on room occupancy, ambient daylight, time of day and task requirements, smart lighting controls could save 70% or more in energy costs compared to non-controlled lighting.

Today, digitalization and the LED lighting revolution have made lighting controls much less costly and complex. At the same time conservation-driven building codes have made them mandatory in most new commercial structures, and increasingly strict local and state energy codes are now requiring these smart control capabilities.

Reduced use of energy is the most obvious gain, but it's a drop in the bucket compared to other potential savings. For instance, when occupancy data from a lighting network is used to optimize space utilization, savings on leasing and provisioning office space can run into hundreds of thousands of dollars a year.

The cell phone provides an apt analogy: when mobile phone manufacturers realized that the device hosting the cellular radio could host any number of sensors, processors, applications and communication technologies, the smartphone revolution transformed our relationship to cyberspace almost overnight.

Today's intelligent LED luminaire is no different: it's a digital device with computing power, connectivity and onboard sensors. Because lighting is ubiquitous, an LED lighting network is an ideal platform to act as a "central nervous system" for smart building management. Thanks to the smartphone industry, a plethora of small, inexpensive sensors and digital devices are readily available to be embedded in LED luminaires. And thanks to various wireless and PoE technologies, those luminaires can connect to and share data with other devices.

As types of IoT devices and API-enabled software continue to expand, the potential 'mash-ups' of data and applications are virtually limitless – just as with your smartphone.

The next step was inevitable: why not link the lighting network to building management systems via BACnet® or something like it? This interoperability means third-party building systems can control the luminaires. It also means that data from the lighting network can be used for fine-tuning HVAC; augmenting security, fire and safety systems; monitoring environmental factors; and interacting with other control systems. And by aggregating data from lighting endpoints onto servers (often cloud-based), sophisticated analytics can be applied for even greater insights and savings. As types of IoT devices and API-enabled software continue to expand, the potential 'mash-ups' of data and applications are virtually limitless – just as with your smartphone.

As a "digital native" devoted solely to LED technology, Cree Lighting recognized from the start that connected lighting networks would require IT-grade security. We have worked hand-in-hand with a well-known global cybersecurity group from day one to build the required security features into the core of our product. In recently completed independent penetration testing, SmartCast® Technology cybersecurity was ranked among the top ten percent of all technology companies tested, which includes the leading technology companies that you use every day.

Visit **creelighting.com/smartcast** or contact a Cree Lighting representative to learn more.

CREE LIGHTING

A COMPANY OF *IDEAL INDUSTRIES, INC.*